Adware/Spyware Removal Procedures

Section 1: Record General Information

Applix #: _____ Date: _____

Technician: _____ Phone: _____

User Name: _____ Org: _____

System Tag #: _____ IP: _____._____._____._____
(run IPCONFIG from DOS)

Section 2: Perform Adware/Spyware Removal

Step	Result
Log in as Administrator	G
Disable Windows System Restore	G
Delete Temporary Internet Files and off-line content	G
Empty Recycle Bin	G
Review MSCONFIG information Disable any suspicious or unknown startup programs Disable any suspicious or unknown services If changes made, reboot	G G G G
Verify anti-virus software status and update as necessary	G
Confirm Tivoli endpoint status and update as necessary	G
Perform a/v software on-demand scan Be sure to activate the unwanted programs detection	G
Were any viruses found? If yes, contact the ASSIST; revert to incident response	Yes / No G
Obtain all a/v logs McAfee logs will be in any of the following locations: C:\Documents and Settings\All Users\Application Data\Network Associates\VirusScan*.txt C:\Documents and Settings\All Users\Application Data\Network Associates\ Common Framework\Db*.txt	G
If applicable, re-image system. System re-imaged? **If yes, skip remaining steps.**	Yes / No
Install Microsoft AntiSpyware	G
Update MSAS signatures	G
Perform MSAS scan	G
Obtain MSAS logs: C:\Program Files\Microsoft AntiSpyware*.gcd	G
Install Ad-aware	G
Update Ad-aware signatures	G
Perform Ad-aware scan	G
Obtain Ad-aware logs: C:\Documents and Settings\<login ID>\Application Data\ Lavasoft\ Ad-Aware\Logs*.txt	G

Install Spybot	**G**
Update Spybot signatures	**G**
Perform Spybot scan	**G**
Obtain Spybot logs: C:\Documents and Settings\All Users\Application Data\ Spybot - Search & Destroy\Logs*.txt	**G**
Was CoolWebSearch found during any scan? If yes, use CWShredder	Yes / No **G**
Remove MS AntiSpyware	**G**
Remove Ad-aware	**G**
Remove Spybot	**G**
Remove any unnecessary/unused programs	**G**
Reactivate Windows System Restore	**G**
Check for and apply any missing Microsoft critical updates	**G**
Does user have Administrator rights? If yes, does user require Administrator rights? If no, remove Administrator rights	Yes / No Yes / No **G**
User log-on successful?	Yes / No
User Web access successful? If no, may need to use LSPFix, WinsockXPFix	Yes / No **G**
Are the spyware symptoms gone? If no, tailored response may be necessary. Escalate to Tier 3 Support or contact the ASSIST Manual removal instructions for some adware/spyware can be found at: http://www.spy-bot.net/manual.asp	Yes / No **G**

If you need assistance at any time, please contact the ASSIST at:

Andrew Cooke, 3-4233; pager, 202-996-4412
or
Josh Knust, 3-4226; pager, 202-539-3808